Ashore AT/FP Vision Brief

Working Class

September 2004

Table of Contents

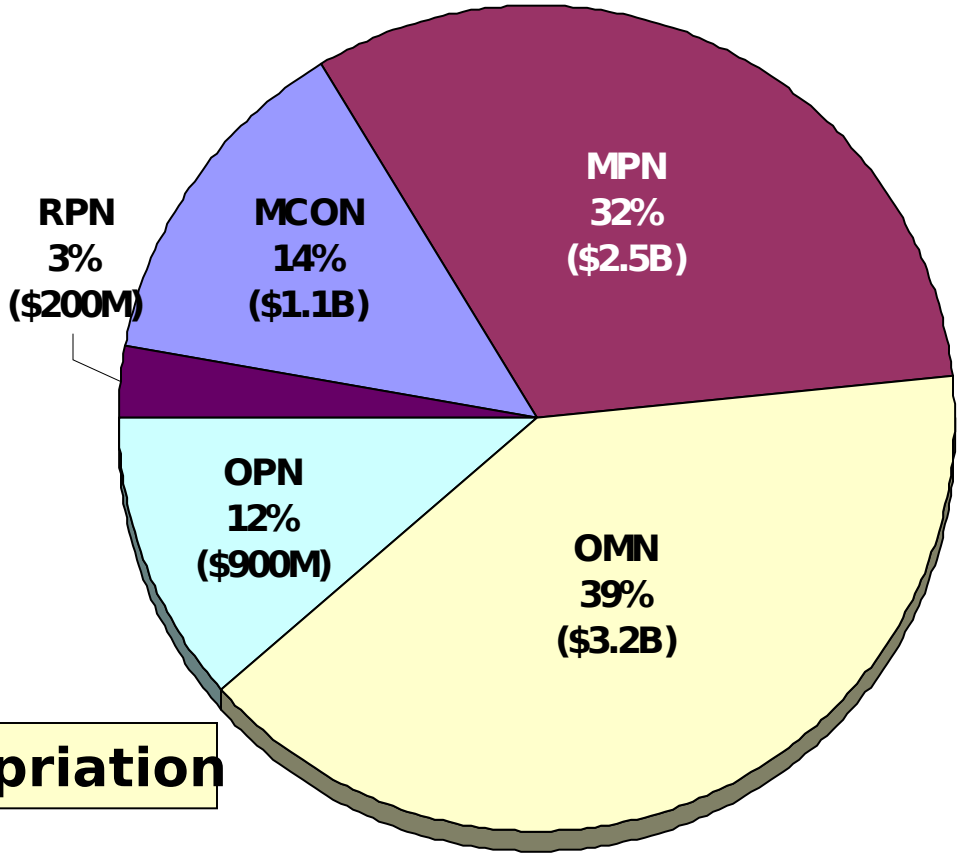
- Situation Today
- Vision
- Strategy
- AT/FP Architecture Development
- Joint/Navy Legacy Programs *"The Purple Band"*
- Ashore AT/FP Program *"The Blue Band"*
- Pilot Programs
- POA&M

In the Past. . .

- **Efforts to date have been installation centric (IMC Driven) and piecemeal without the benefit of a single overarching Navy Ashore vision.**
- **SYSCOMs not participating in fastest growing program from 9/11**
- **DERF FP Procurements lack sustainment and logistical support**
- **Six separate CBRN fielding programs lack alignment**

Current Approach- "Risk Aversion": Prohibitive Cost, Slow Implementation, Unrealistic Resourcing—UNACHIEVABLE!

Ashore Combating Terrorism Resource



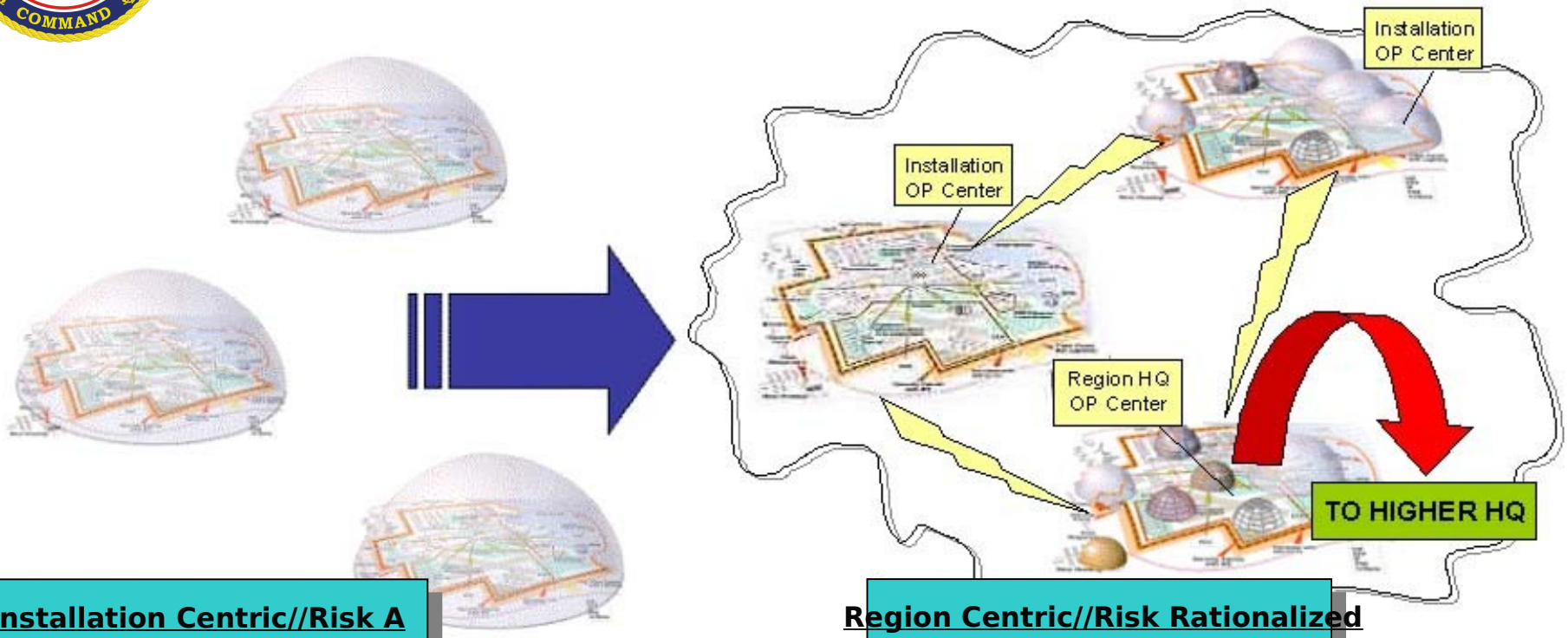
Total = $7.9B
(FY05-09)

Appropriation

CNI's Vision for Implementing AT/FP at Shore Installations

- **Formalized Framework**
- **Region Centric**
- **Capabilities Based**
- **Risk-Rationalized Approach**

Now. . .Future



Installation Centric//Risk A version

- Accepts No Risk, Unachievable
- Slow Implementation, Increases Risk
- Prohibitive Cost
- Unrealistic Resourcing
- DoD/Joint Vision
- Lacks Sustainment

Region Centric//Risk Rationalized

- Accepts Some Risk
- Implement More Quickly
- Balance Resources Based on Navy Capability Gaps, Criticality, Vulnerability, Threat and Comparative Advantage
- Formalized Framework

Strategy

- **Align programs using Joint and General Accounting Office (GAO) guidance**
- **Senior Steering Group (SSG)/SYSCOM Antiterrorism Team (SAT) Process**
  - **Requirements Generation**
  - **Resource/Programming**
  - **Execution**
  - **FFC Advisory Role**
- **Refine FFC/CNI Requirements Identification Process**
- **Fully Realize Public Safety Shore Installation Model starting with Pilot Program development and execution**
- **Implement Risk-Based Investment Strategy**
- **Develop Region-Centric Programs of Record to include sustainment**

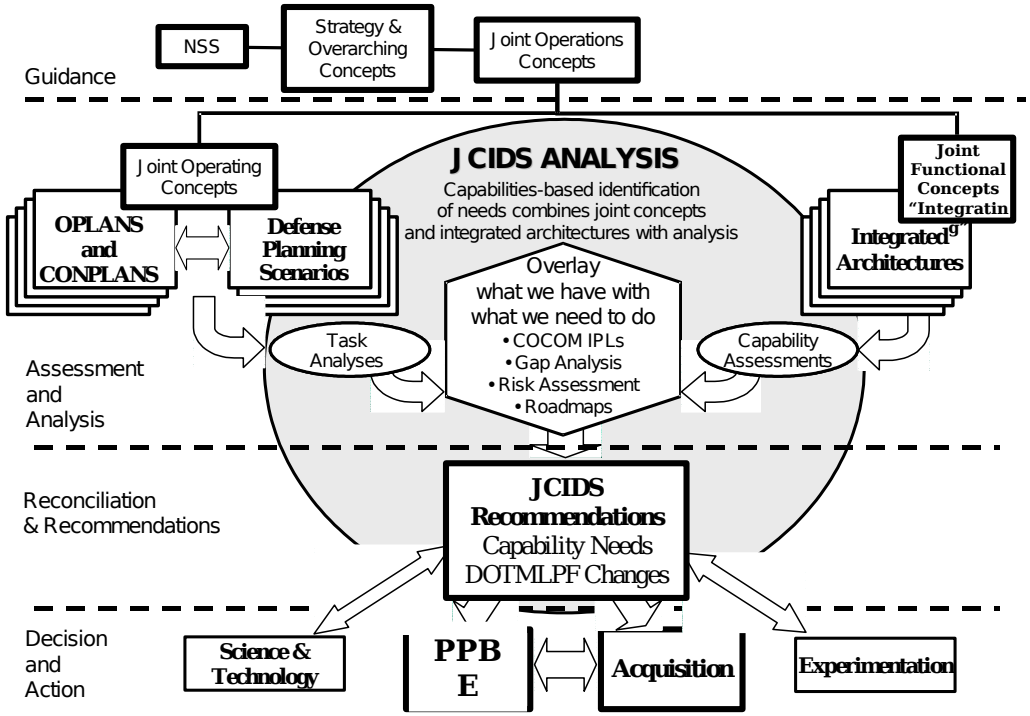
Development of Ashore AT/FP Program Process

Basic Tenets

- **Joint Capabilities Integration Development System (JCIDS)**
  - **Joint concept centric capability identification process**
  - **Assess existing and proposed capabilities**
  - **Deliver technologically sound sustainable and affordable increments of capability**
  - **Aligns AT Ashore with the JS Protection FCB**

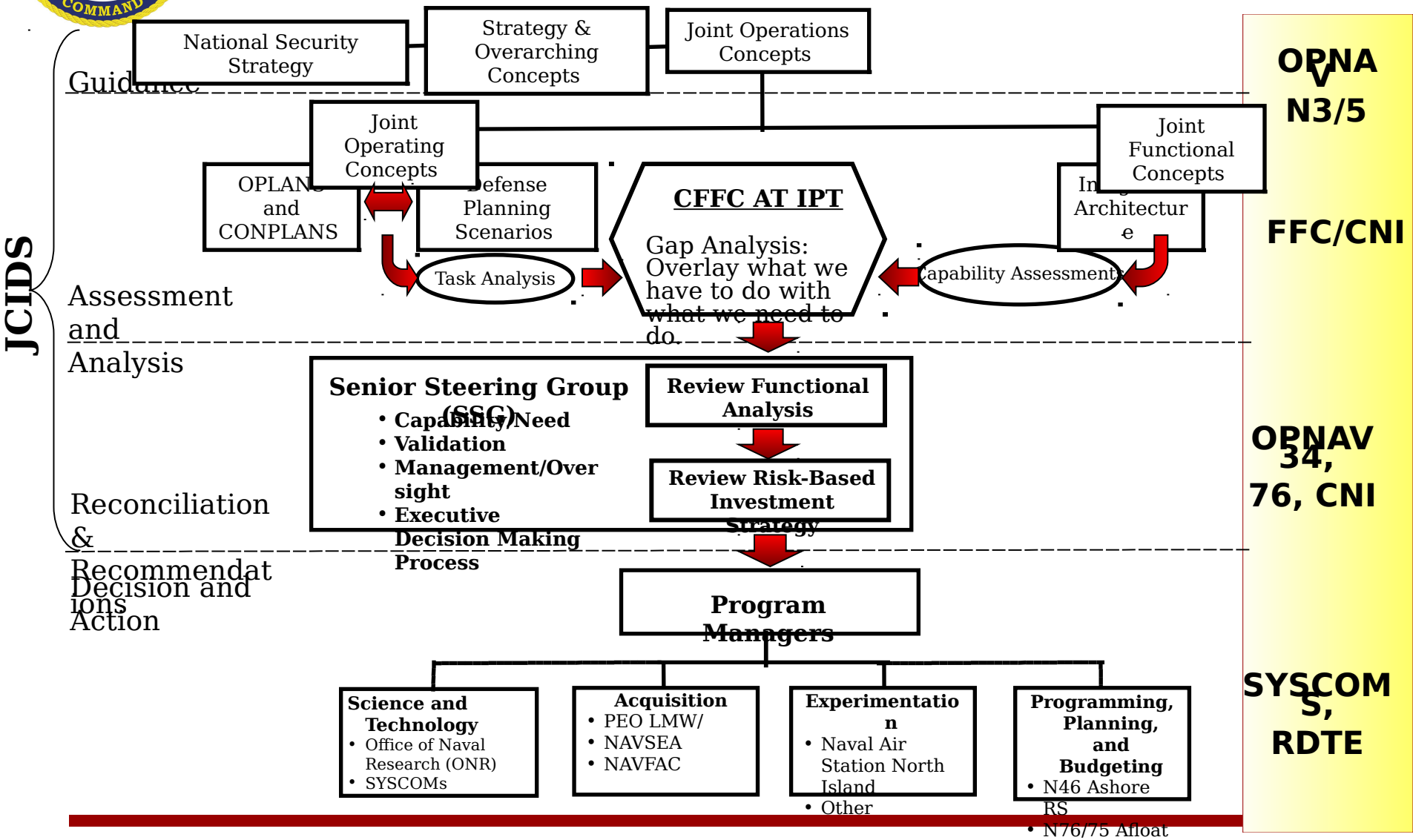
Joint Capability Integration and Development System (JCIDS)

- Based on the need for joint forces to meet security challenges in the future through flexible, distributed and highly networked operations.
- Transforms and implements a process that assesses legacy and proposed systems and defines desired joint capabilities.
- Considers the most effective joint force capabilities and integrates those capabilities early in the acquisition process.



- *JCIDS supercedes CJCSI 3170.01B and DJSM-0921-02.*
- *Required by DoD Instruction 5000.2, CJCSI 3170.01C. (RGS)*

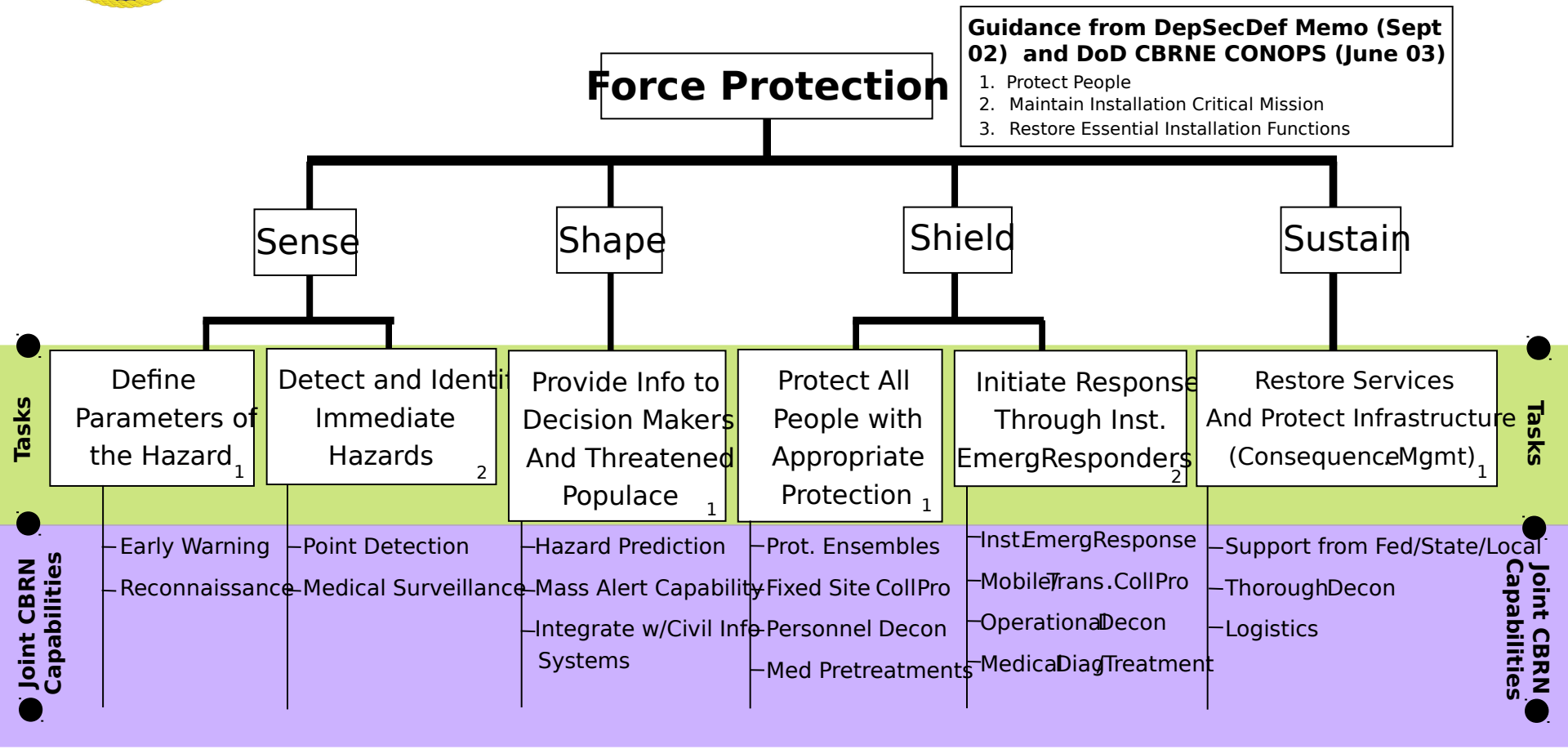
AT/FP Capabilities & Integration Process



DoD Proposed Ashore AT/FP Architecture

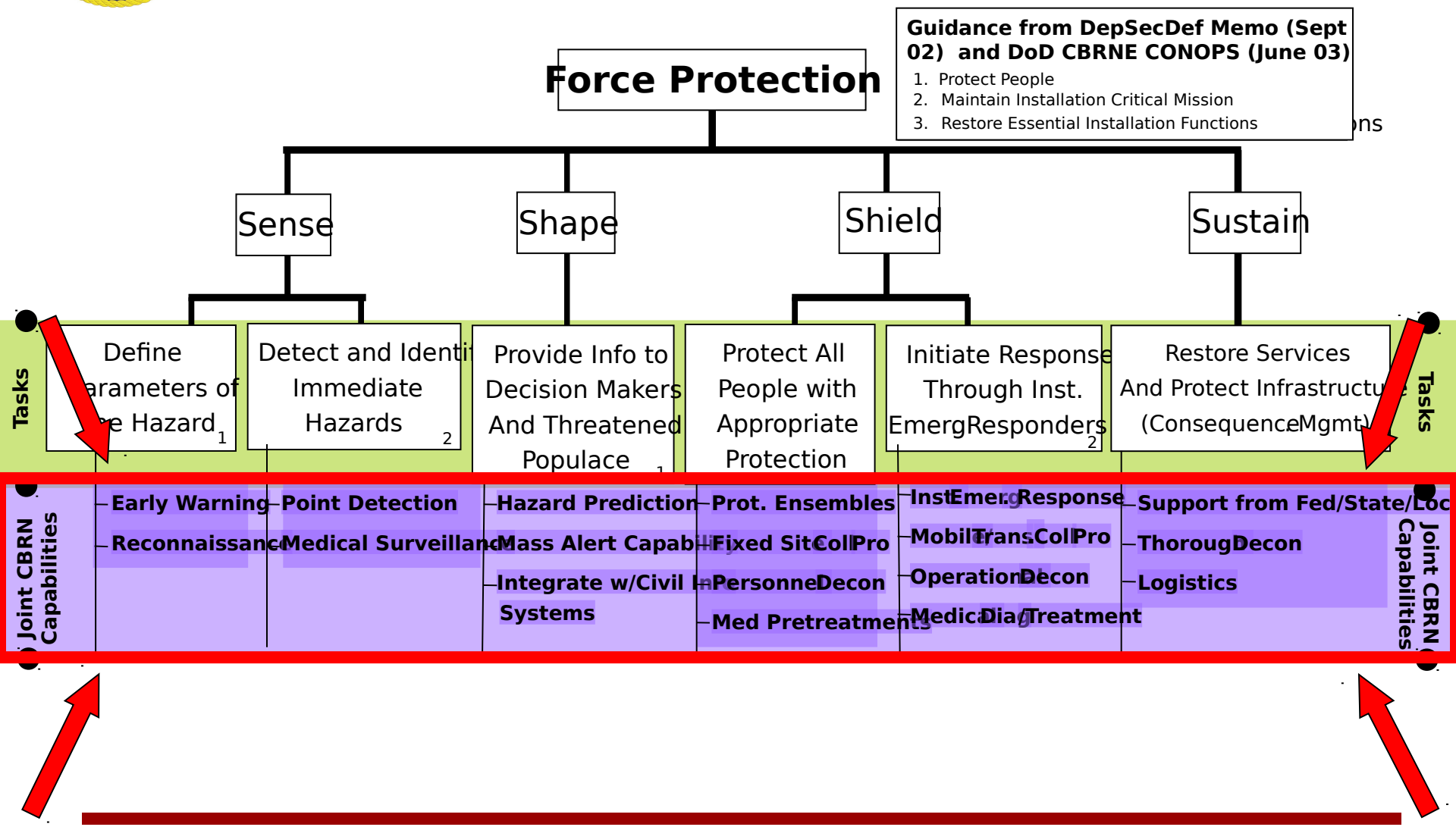
Guidance from DepSecDef Memo (Sept 02) and DoD CBRNE CONOPS (June 03)

1. Protect People
2. Maintain Installation Critical Mission
3. Restore Essential Installation Functions



Implementation of Joint/Navy Legacy CBRN Programs

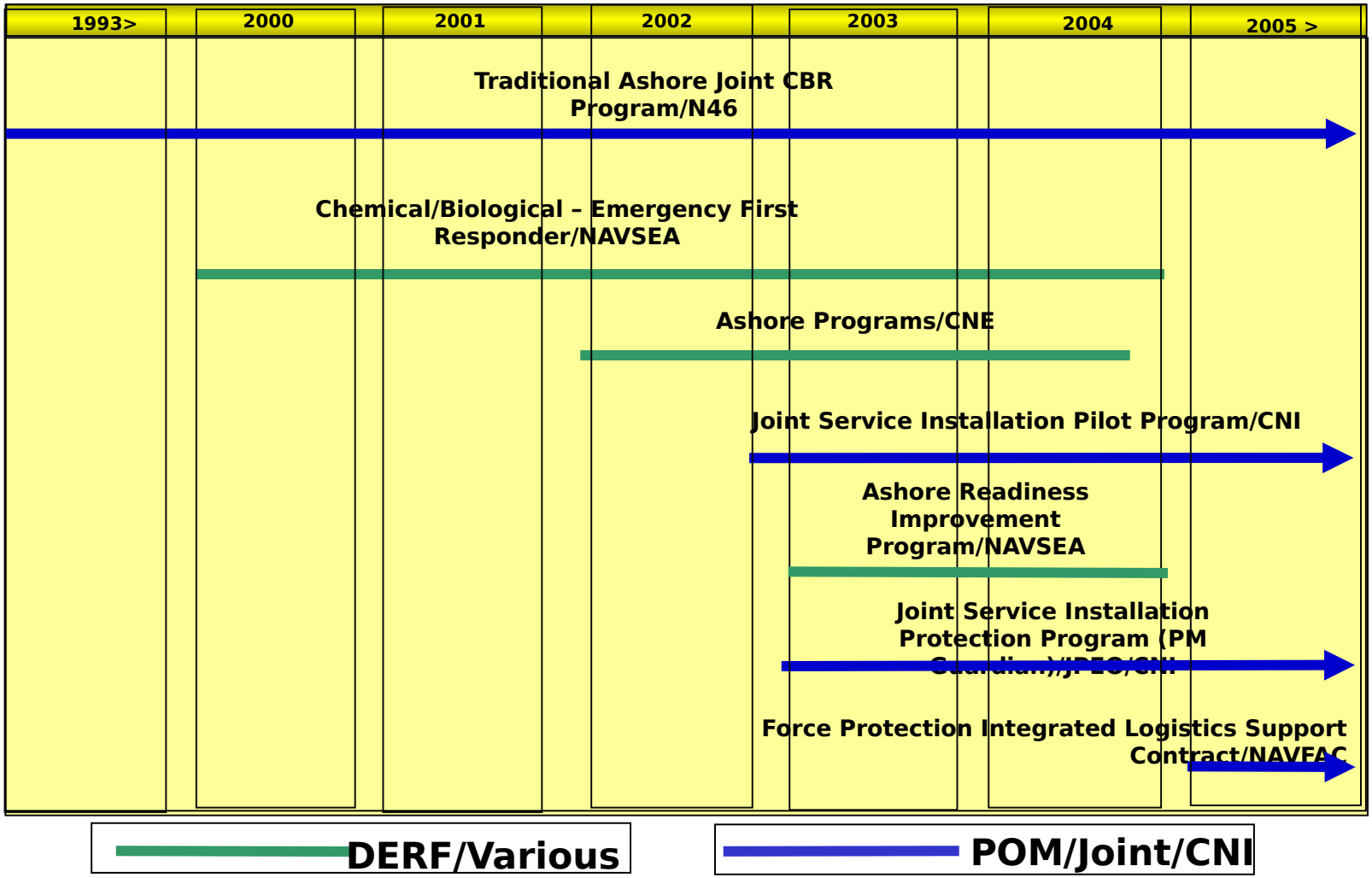
"The Purple Band"



Current Joint/Navy Legacy CBRN Programs

- **Six separate fielding programs**
  - Traditional Ashore Joint CBR Program
  - Chemical/Biological – Emergency First Responder
  - Ashore Programs
  - Ashore Readiness Improvement Program
  - Joint Service Installation Pilot Program
  - Joint Service Installation Protection Program (PM Guardian)
- **One logistics program**
  - Integrated Logistics Support Contract

CBRN Programs

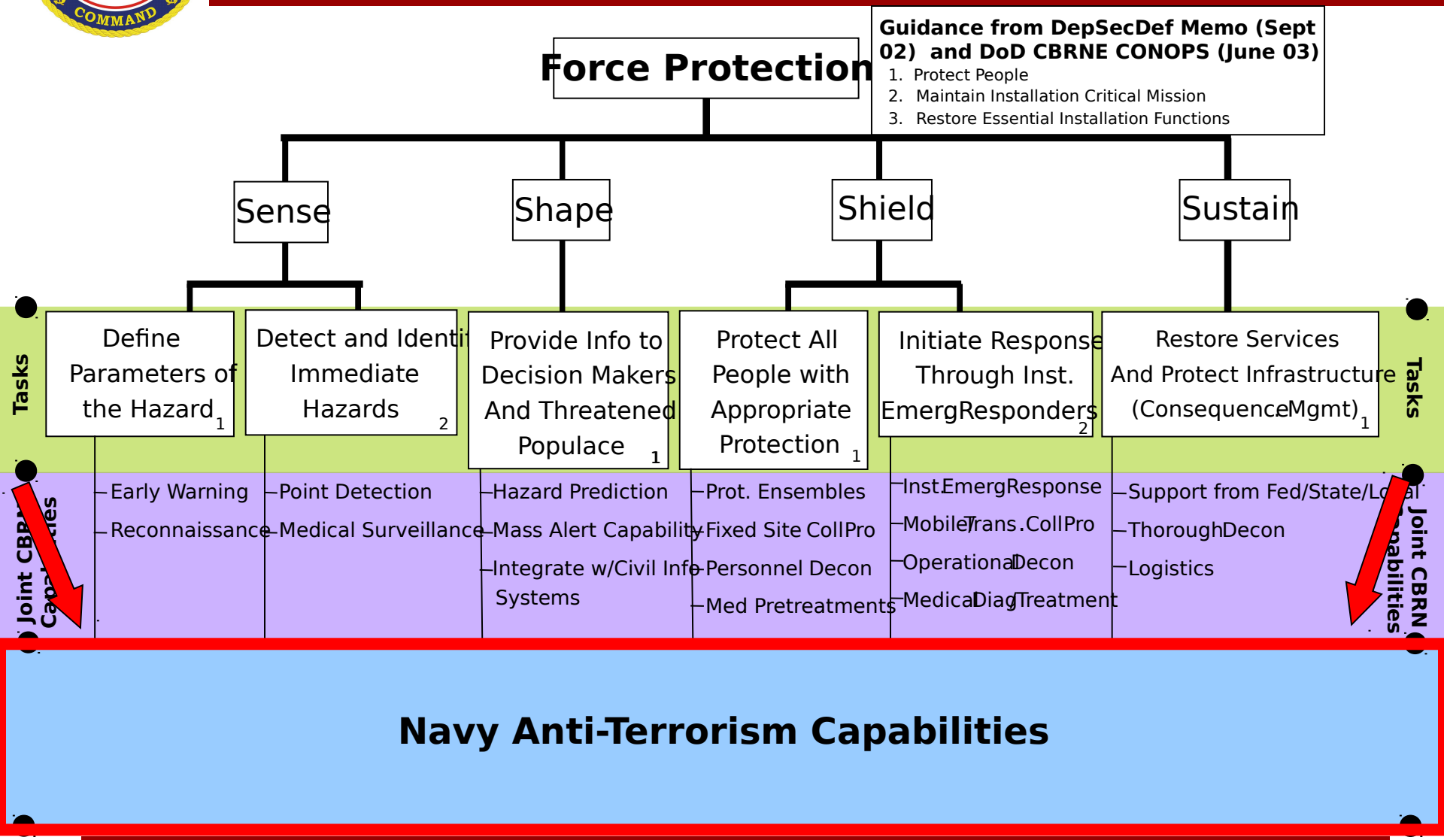


CNI Public Safety Strategy for Joint Programs

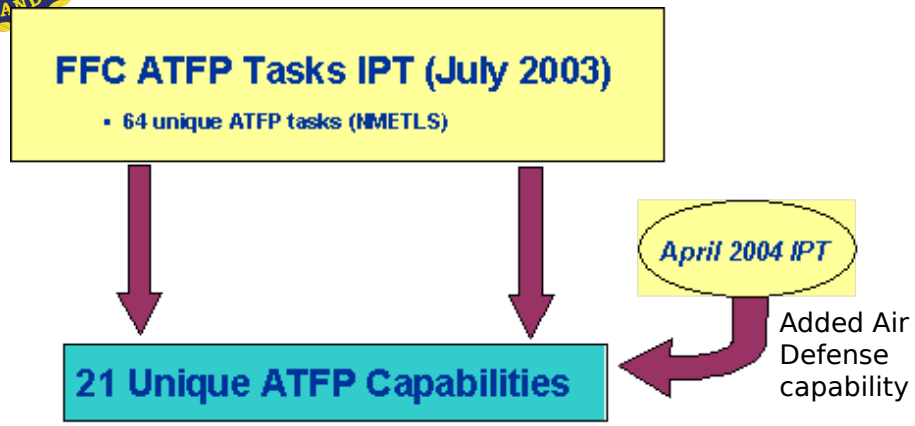
- **Satisfy Joint Staff Guidance** — Y
- **Align with CB Ashore programs** — G
- **Establish Life Cycle Management** — Y
- **Sustainable and Standardized** — G
- **Assess/quantify impacts of all CBRN equipment being delivered through joint programs (“The Purple Band”) to Regions/Installations to define/de-conflict requirements for Risk Rationalized AT/FP Plan (“The Blue Band”)** — G

Development and Implementation of Ashore AT/FP Program

"The Blue Band"



CFFC Program Guidance/Priority


FFC ATFP Tasks IPT (July 2003)
• 64 unique ATFP tasks (NMETLS)
April 2004 IPT
Added Air Defense capability
21 Unique ATFP Capabilities

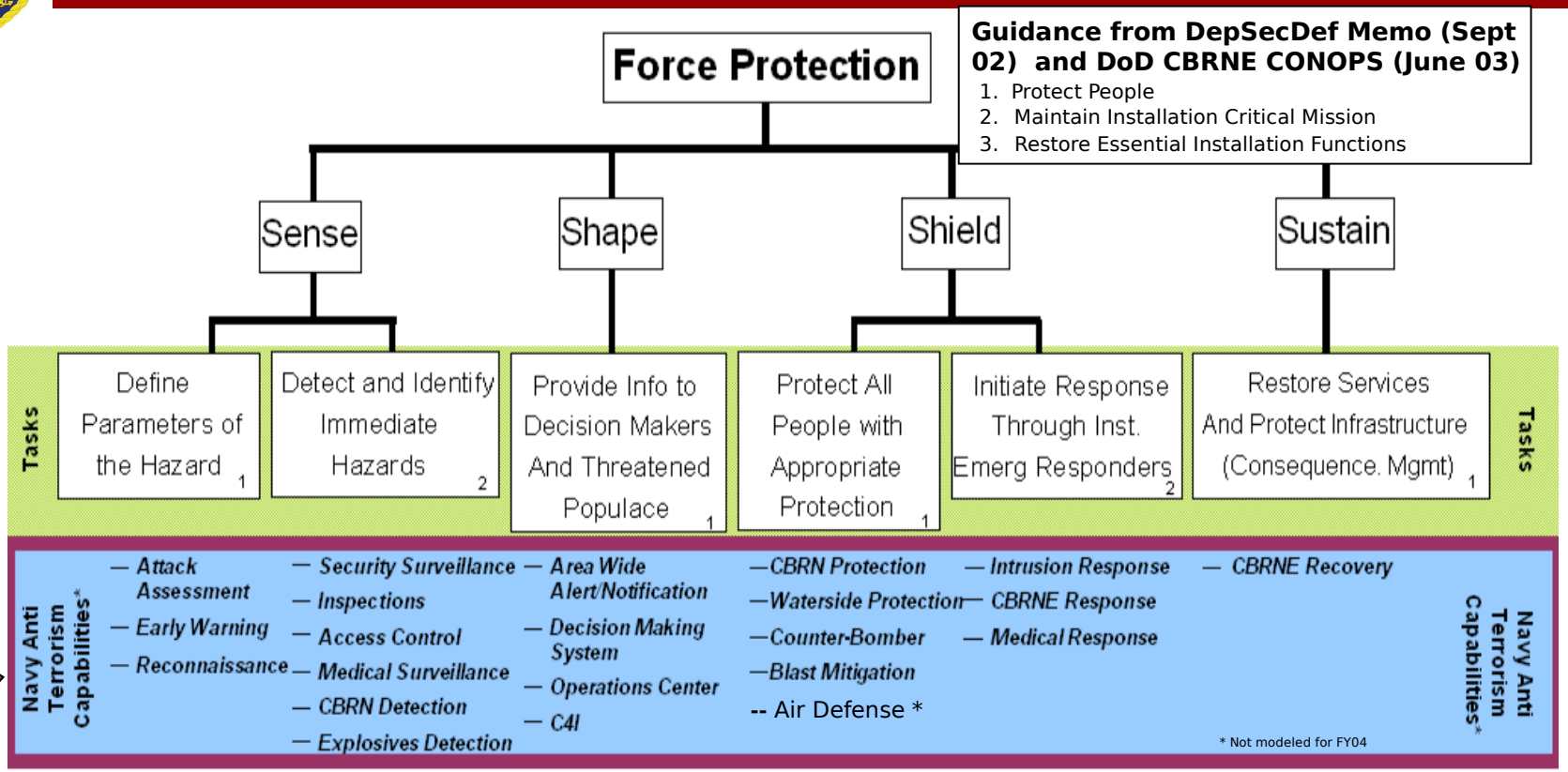
Development and Implementation of Ashore AT/FP Program

"CFFC (4-Star) Intent"

- **Establish and Optimize Cost Effective AT Capabilities**
- **Manage CBRN Expenditures in Support of Joint Programs**
- **Pursue Capability Pilot Projects for Implementation**
  - **Information Management & Base-Wide Alert**
  - **Physical Security/Access Control**
- **Identify Full-Spectrum Capabilities to Facilitate Training, Exercise, and Reporting Requirements**
- **Align AT/FP Capabilities around FFC Requirements IPT Process**

Development and Implementation of Ashore AT/FP Program

"The Blue Band"



- **22 Unique Navy Ashore AT/FP Capabilities were developed based on NMETLS at the FFC AT/FP Tasks IPT (July 2003)**
- **Navy Ashore AT/FP Capabilities were validated at the FFC AT/FP Requirements IPT (April 2004)**

Development of CNI Risked Based Model

Assumption

Risk can be analyzed using: Threat, Vulnerability and Criticality

Threat

- –What threats exist today and what is the relative likelihood of each threat?
- –How would the likelihood of the threat change by investing in specific antiterrorism capabilities?

Vulnerability

- –If an attack were attempted, what is the likelihood that it is successful?
- –By implementing a specific Force Protection capability, what level of reduction in vulnerability to an attack of this type can be expected?

Criticality

- –If an attack occurs and is successful, what are the consequences to:
  - ➢People
  - ➢Assets and Infrastructure
  - ➢Mission Capability
- –By implementing the specific Force Protection capability, what level of reduction in criticality can be expected?

CNI Risked Based Model

Fleets with CNI

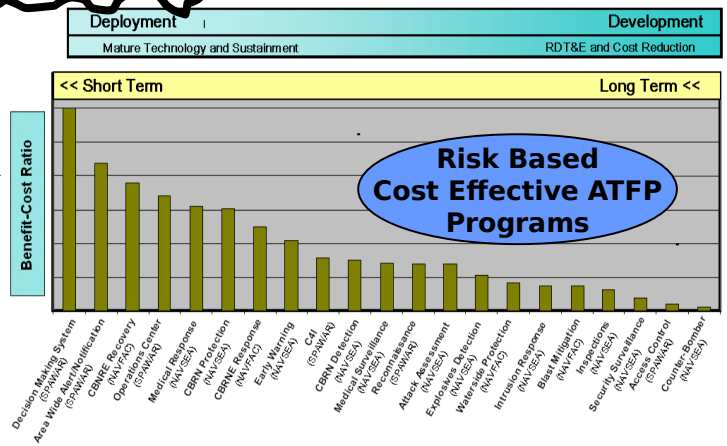
- Threats
- Vulnerabilities
- Criticalities
- Capabilities

Threat type	Target	Criticality: People	Criticality: Economic	Criticality: Mission	Baseline	Risk Impact of AT Capability: Attack Assessment	Early Warning	Reconnaissance	Security Surveillanc	Inspections	Access Control	Medical Surveillance	CBRN Detection	Explosives Detectio	Area Wide Alert/Notification	Decision Making Sy
Land	Personnel															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Land	Structures															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Land	Vessels and aircraft															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Land	CIP															
	Relative Threat:															
	Vulnerability:															
	Criticality:															
Sea	Personnel															
	Relative Threat:															
	Vulnerability:															
	Criticality:															

Risk Based Investment Strategy

SALT

- Technology Maturity
- Deployability



$$= \frac{\left[\text{Risk}(T/V/C)_{\text{Baseline}} - \left[\text{Risk}(T/V/C)_{\text{WithAT Capability}}\right] \times (TF) \times (DF)\right.}{\text{Navy Cost of the AT Capability}}$$

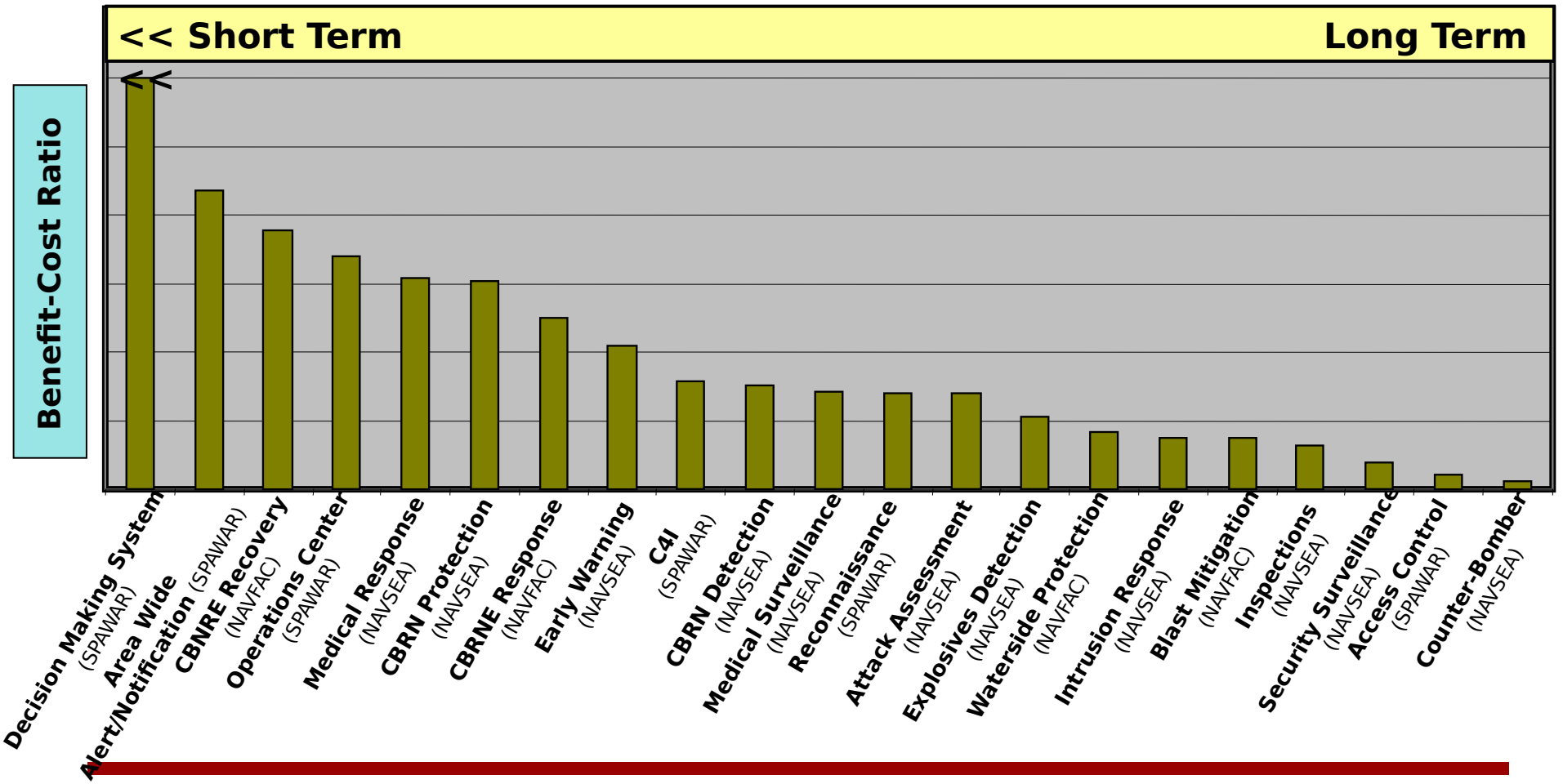
Risk(T/V/C) = Risk measured as a function of Threat, Vulnerability, and Criticality
TF = Technology maturity factor
DF = Deployability factor

CNI Risk Based Model

AT/FP Capabilities Relative Ranking of Benefit-Cost

Deployment effectiveness | **Development efficiency**

Mature Technology & Sustainment | **RDT&E & Cost Reduction**



Capability Area Framework

Sense

Attack Assessment - SEA
Name/Org: Ray Campfield / NSWCDD (CBR)
Telephone: (540) 653-5249
Email: CampfieldRF@nswc.navy.mil

Early Warning - SEA
Name/Org: Dusty Wilson / NSWC Crane
Telephone: (812) 854-5447
Email: Wilson_Dustin@crane.navy.mil

Reconnaissance - SPA
Name/Org: John Mitchell / SPAWAR SD
Telephone: (619) 524-2080
Email: john.w.mitchell@navy.mil

Security Surveillance - SEA
Name/Org: Dusty Wilson / NSWC Crane
Telephone: (812) 854-5447
Email: Wilson_Dustin@crane.navy.mil

Access Control - SPA
Name/Org: Phil Bailey / SPAWAR CH
Telephone: (843) 218-5565
Email: philip.bailey@navy.mil

CBRN Detection - SEA
Name/Org: Ray Campfield / NSWCDD (CBR)
Telephone: (540) 653-5249
Email: CampfieldRF@nswc.navy.mil

Shape

Area Wide Alert/Notify - SPA
Name/Org: Tom Charters / SPAWAR SD
Telephone: (619) 553-4864
Email: tom.charters@navy.mil

Decision Making System - SPA
Name/Org: Phil Bailey / SPAWAR CH
Telephone: (843) 218-5565
Email: philip.bailey@navy.mil

Operations Center - SPA
Name/Org: Phil Bailey / SPAWAR CH
Telephone: (843) 218-5565
Email: philip.bailey@navy.mil

C4I - SPA
Name/Org: Tom Tiernan / SPAWAR SD
Telephone: (619) 553-3562
Email: tom.tiernan@navy.mil

Inspections - SEA
Name/Org: Dave Acton / NSWC Crane
Telephone: (812) 854-5726
Email: Acton_D@crane.navy.mil

Medical Surveillance - SEA
Name/Org: Ray Campfield / NSWCDD (CBR)
Telephone: (540) 653-5249
Email: CampfieldRF@nswc.navy.mil

Explosives Detection - SEA
Name/Org: Chris O'Donnell / EODTECHDIV
Telephone: (301) 744-6850 x 262
Email: odonnell@eodpoe2.navsea.navy.mil

Shield

CBRN Protection - SEA
Name/Org: Ray Campfield / NSWCDD (CBR)
Telephone: (540) 653-5249
Email: CampfieldRF@nswc.navy.mil

Waterside Protection - FAC
Name/Org: Bob Taylor / NFESC
Telephone: (805) 982-5914
Email: Robert.Taylor5@navy.mil

Counter-Bomber - SEA
Name/Org: Chris O'Donnell / EODTECHDIV
Telephone: (301) 744-6850 x 262
Email: odonnell@eodpoe2.navsea.navy.mil

Intrusion Response - SEA
Name/Org: Steve Gorin / NSWCDD CSS
Telephone: (850) 235-5516
Email: gorinse@ncsc.navy.mil

CBRNE Response - FAC
Name/Org: Peter Novick / NAVFAC HQ
Telephone: (202) 685-9209
Email: Peter.Novick@navy.mil

Medical Response - SEA
Name/Org: Ray Campfield / NSWCDD (CBR)
Telephone: (540) 653-5249
Email: CampfieldRF@nswc.navy.mil

Blast Mitigation - FAC
Name/Org: Jim Tancreto / NFESC
Telephone: (805) 982-1180
Email: James.Tancreto@navy.mil

Air Defense - AIR
Name/Org: Brandy Flotten / NAVAIR
Telephone: (773) 324-7237
Email: brandy.flotten@navy.mil

Sustain

CBRN Recovery - FAC
Name/Org: Peter Novick / NAVFAC HQ
Telephone: (202) 685-9209
Email: Peter.Novick@navy.mil

Red= NAVSEA (non-CBR)

Grey = NAVSEA (CBR)

Yellow = SPAWAR

Blue = NAVFAC

Green = NAVAIR

Required Operational Capabilities (ROCs)

1- Strategic Asset or High Threat Bases

(a) Provides protection for nuclear weapons and supporting systems (SSBNs). Staffed to support current DoD (41M) security requirements.

(b) Requires special protection requirements due to their high threat environment. Tailored staffing to support fulltime C/D.

2 - Operational Bases (OB) and critical C4ISR

- Major fleet homeports home-ported combatant ships and/or tactical aircraft; forward operating locations (OCONUS); critical load-out/ embarkation stations; and critical C4ISR communication stations.

3 - Sustainment & Support Activities (S&SA)

(a) Sustainment - Hospitals, bases with non-combatant ships, non-tactical aircraft, weapons storage facilities, logistics sites, shipyards & maintenance facilities.

(b) Support - headquarters, and communication sites; and includes any enclave area associated with ROC 2 bases.

4 - Administrative and Training Activities (A&TA)

- Reserve bases; R&D centers; administrative facilities/complexes, i.e. BUPERS Millington; recreational areas and MWR facilities; exchanges and commissaries; training sites, e.g. Naval Academy and Staff Colleges; museums and displays like the USS Constitution; and includes any enclave area associated with ROC 2 or 3 bases.

DoD Concepts of Operation for Chemical, Biological, Radiological, Nuclear, and and High-Yield Explosive (CBRNE) Defense Supporting Military Installation and Facility Preparedness, February 2004

Linking ROCs and CLs
with Notional Regional Overlay

The 4X4 matrix

OBJECTIVES

- Better linking of resources to output
- Enhances costing at various levels of performance
- Improves linkage between mission requirements, known capabilities, and performance
- Better aligns product and service delivery with warfighter/customer expectations
- A better assessment of capability versus requirement supporting management of risk.

✓Ensure Standards

Capability Levels (CLs)

Required Operational Capabilities* **(ROCs)**

ROC ↓	CL 1	CL 2	CL 3	CL 4
1	KINGS BAY			
2			KEY WEST MAYPORT	
3			MERDIAN ATLANTA	
4			ATHENS	

NOTIONAL

$$\text{Productivity} = \frac{\text{Output}}{\text{Cost}}$$

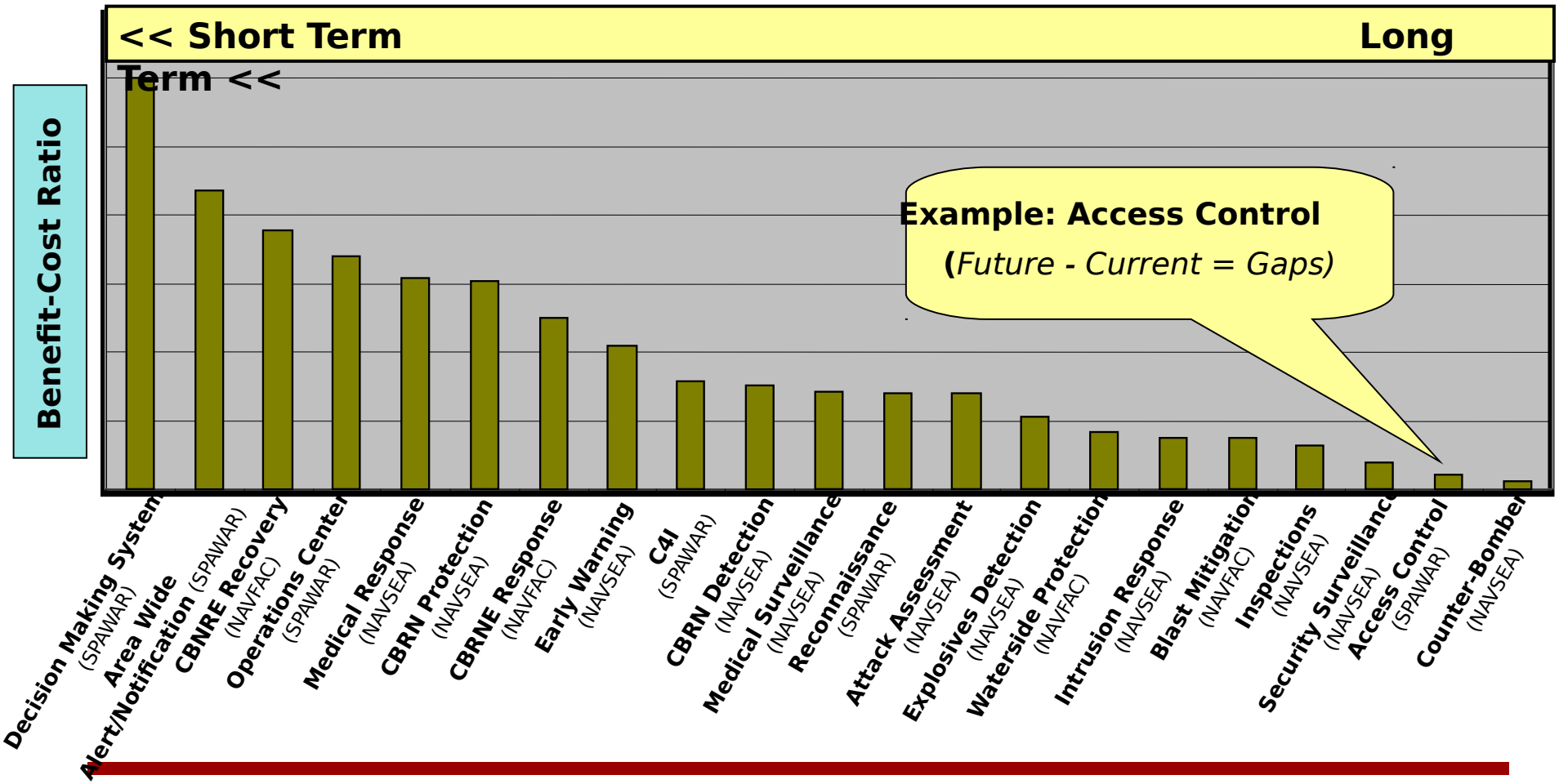
* Joint Staff Installation & Facility Preparedness Guidance (2

CNI Risk Based Model

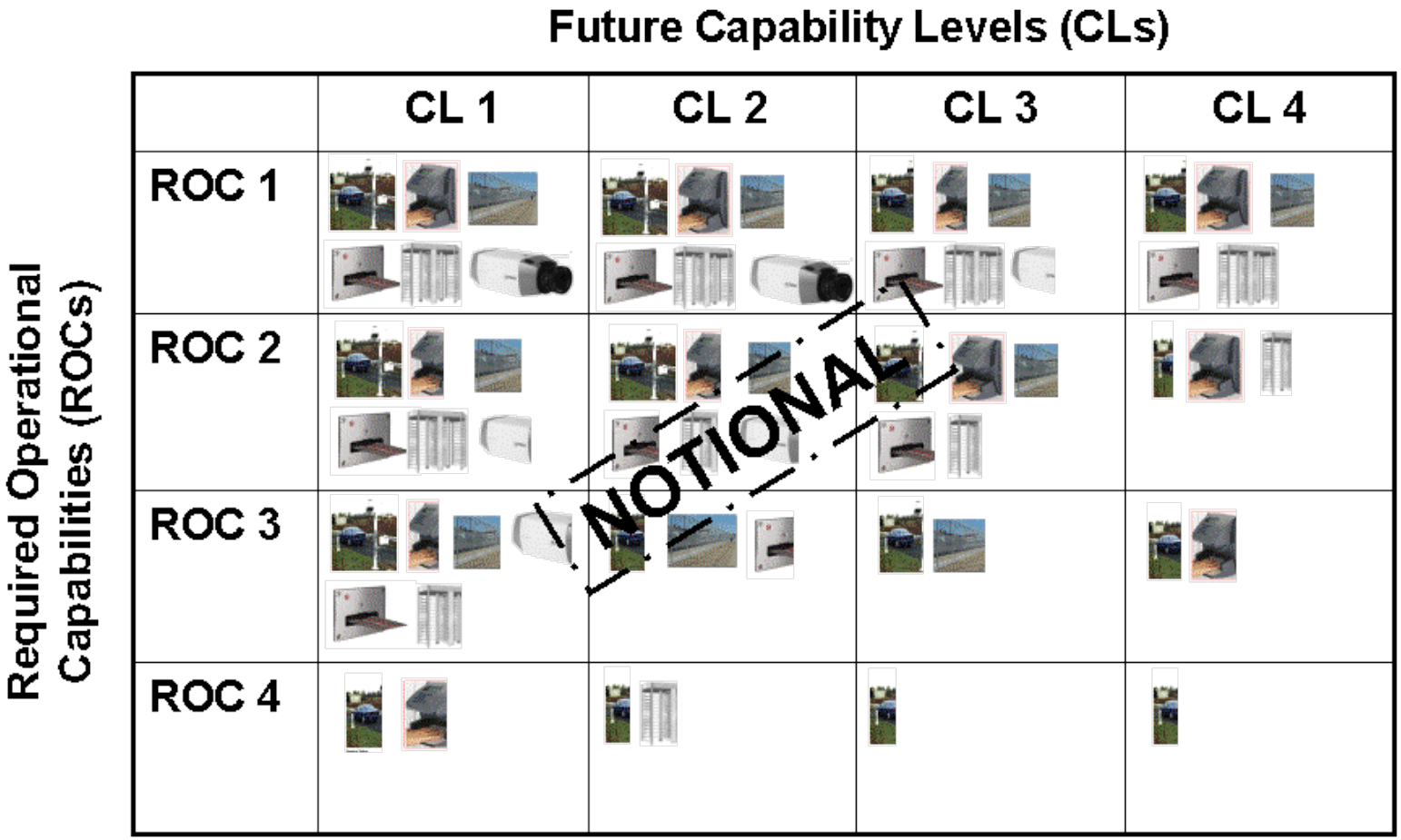
AT/FP Capabilities Relative Ranking of Benefit-Cost

Deployment effectiveness — **Development efficiency**

Mature Technology & Sustainment — **RDT&E & Cost Reduction**



Access Control Notional Capability (Future)

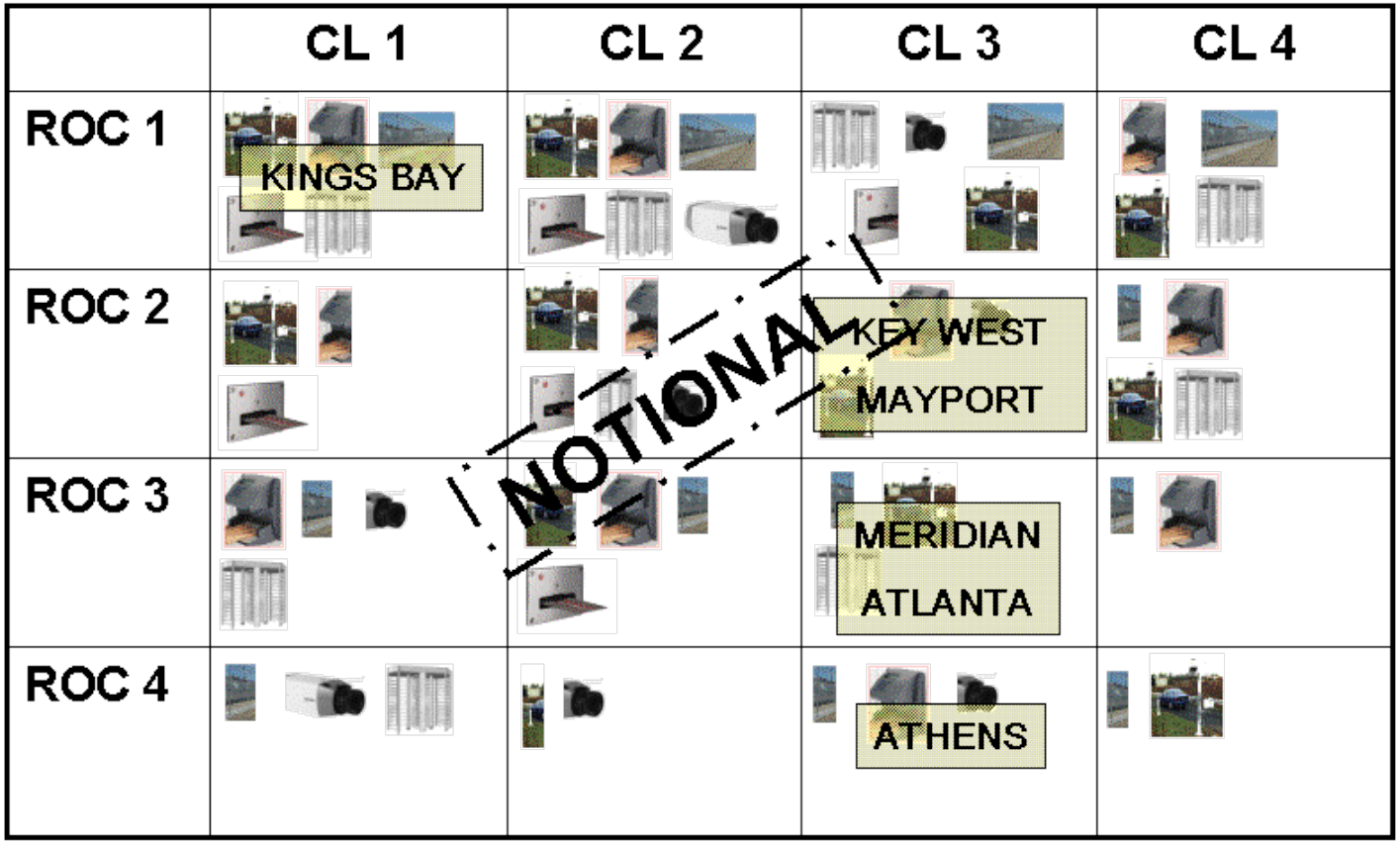


Access Control Notional Capability (Current)

with Notional Regional Overlay

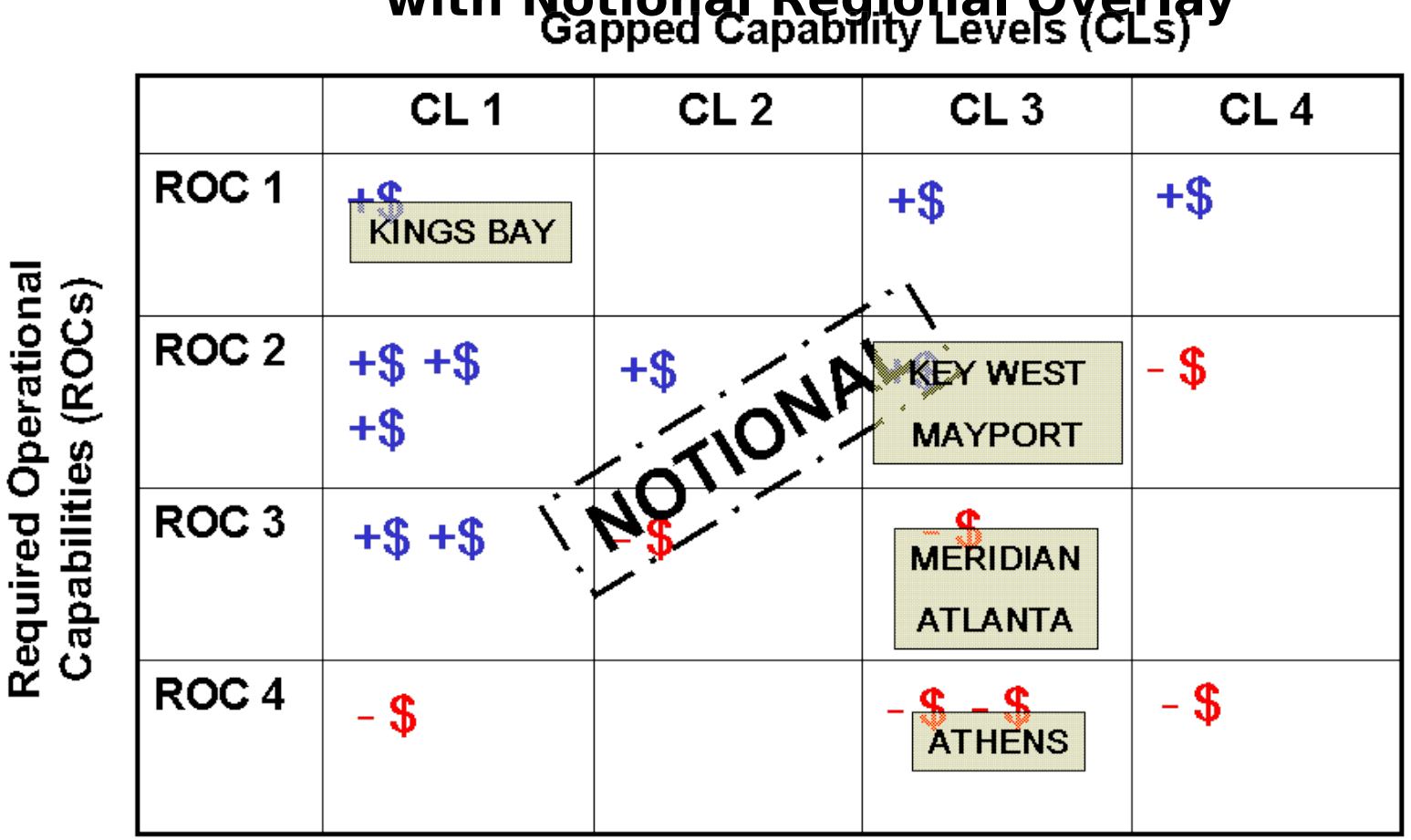
Actual Capability Levels (CLs)

Required Operational Capabilities (ROCs)



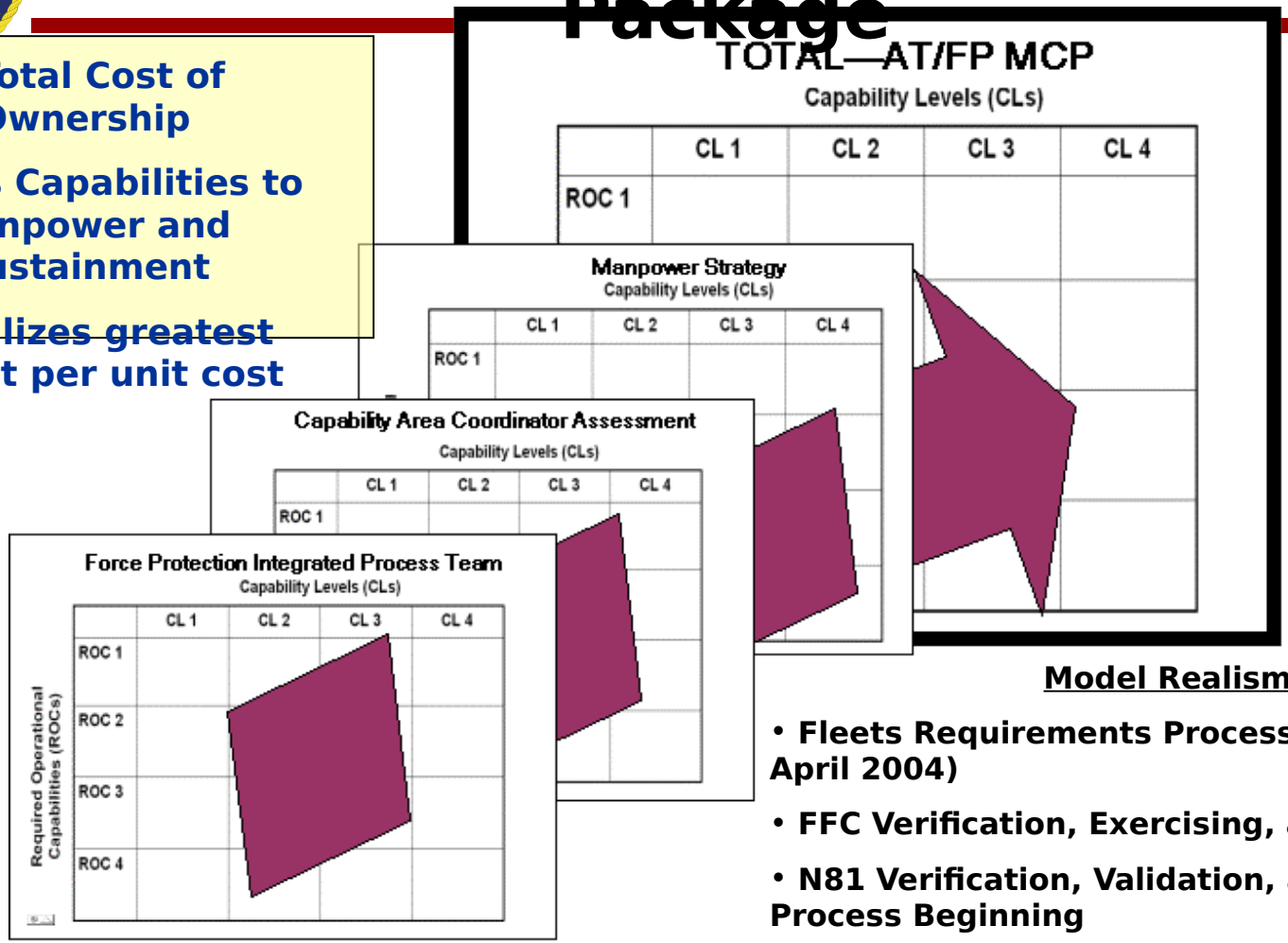
Access Control Notional Capability (Gaps)

with Notional Regional Overlay



Ashore AT Capabilities Package

- **Total Cost of Ownership**
- **Links Capabilities to Manpower and Sustainment**
- **Realizes greatest output per unit cost**



Model Realism

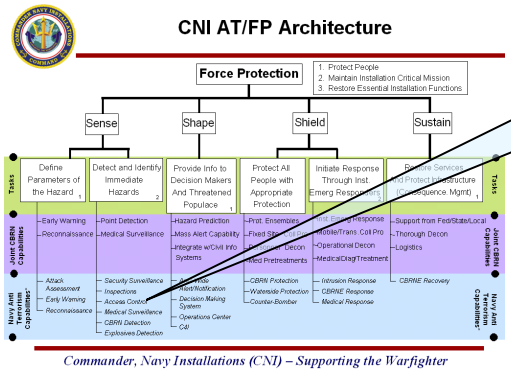
- **Fleets Requirements Process (July 2003 & April 2004)**
- **FFC Verification, Exercising, and SORTS**
- **N81 Verification, Validation, and Analysis Process Beginning**

Intangibles Captured

- **SAT/SYSCOM Execution Guidance by CNI**

Shore Program Centric Solutions

Moving away from installation centric AT/FP solutions *... to Program Centric AT/FP Solutions.*



Access Control

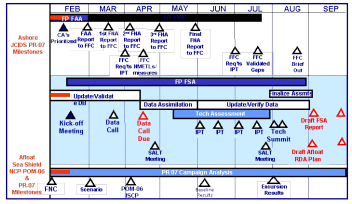
Via CNI w/ SAT

NAVFAC Program Manager

+

N46/CNI Resourcing FYDP

+



Technology Roadmap (Under Development)

+

FFC IPT Tasks/ (NMETLS)

Program Managers Guide

Program Managers Strategic Elements of Success

- Risk Management Principals applied to decision making
- Solutions result in the elimination of personnel and process layering/duplication
- Rationalized, cost reduction of AT/FP accounts
- Improved service delivery without increased cost
- Optimization/rationalization of technology with processes & personnel
- Leverage Joint/Interagency/Other Services Processes and Resources
- Non material solutions (JCIDS DOTMLPF)
- Use of Operational Deception
- Other Intangibles (e.g. traffic delay, employee satisfaction…)

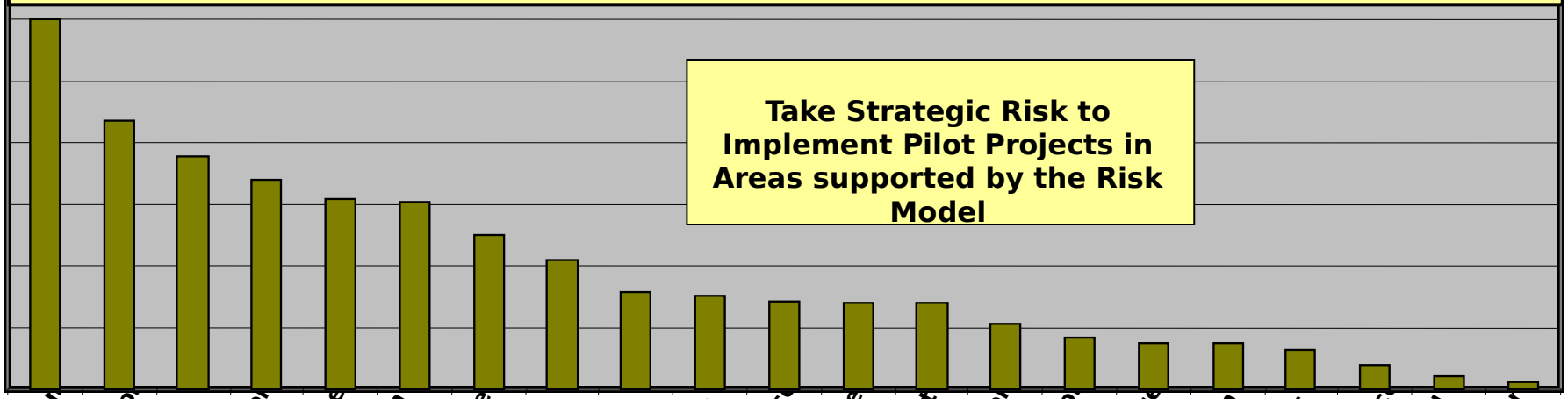
CNI Risk Based Investment Model

Deployment effectiveness | **Development efficienc**

Mature Technology & Sustainment | **RDT&E & Cost Reduction**

<< Short Term | **Long Term <<**

Benefit Cost Ratio



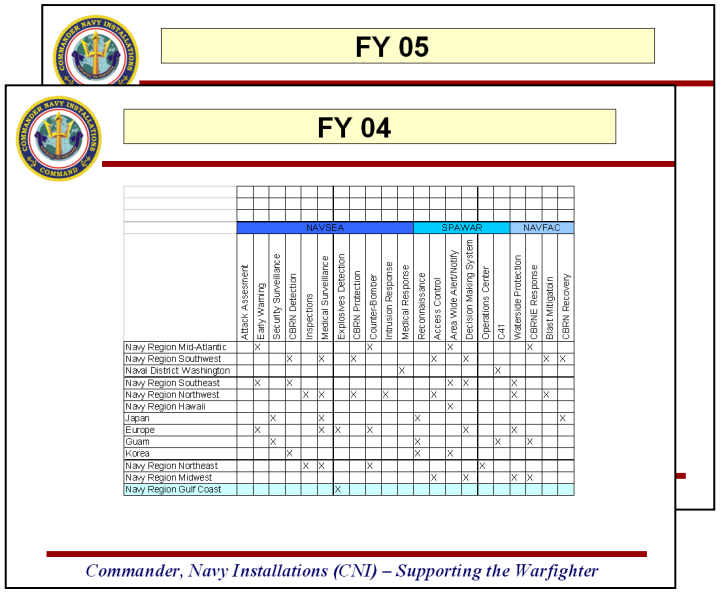
Decision Making Syste (SPAWAR)
Area Wide Alert/Notificatio (SPAWAR)
CBNRE Recovery (NAVFAC)
Operations Cente (SPAWAR)
Medical Response (NAVSEA)
CBRN Protection (NAVSEA)
CBRNE Response (NAVFAC)
Early Warning (NAVSEA)
C4I (SPAWAR)
CBRN Detection (NAVSEA)
Medical Surveillanc (NAVSEA)
Reconnaissance (SPAWAR)
Attack Assessment (NAVSEA)
Explosives Detectio (NAVSEA)
Waterside Protectio (NAVFAC)
Intrusion Response (NAVSEA)
Blast Mitigation (NAVFAC)
Inspections (NAVSEA)
Security Surveillanc (NAVSEA)
Access Control (SPAWAR)
Counter Bomber (NAVSEA)

Pilot Projects for FY04-05

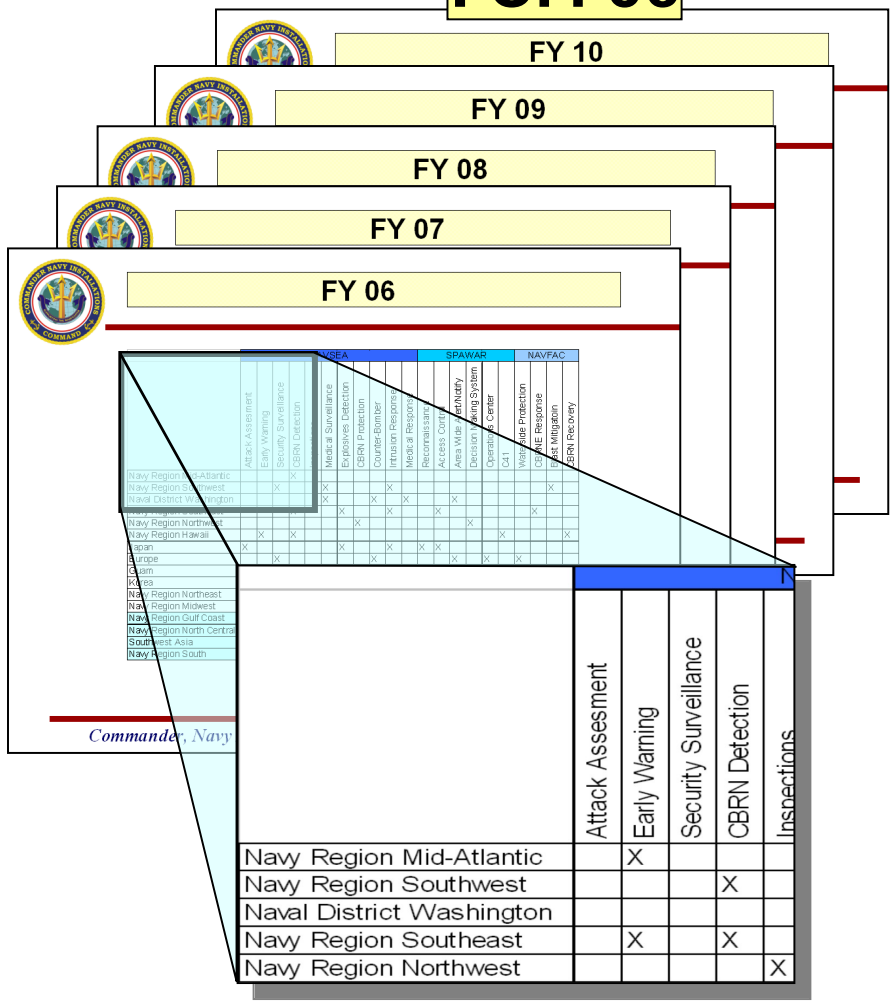
nformation Management & Base Wide Ale | **Physical Security/Access Contro**

Development and Implementation of Shore AT/FP Programs

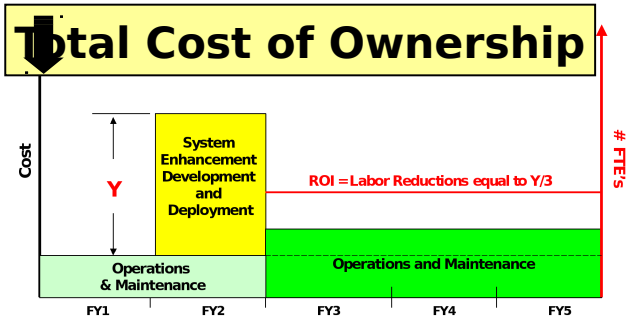
Pilot Programs



POM 06



Total Cost of Ownership



AT/FP Investment in Pilot Programs

	Information Management & Base Wide Alert		Physical Security / Access Control Pilot			
Location	**CNRMA**		**CNRSE**		**CNRSW**	
	Cost	**Date**	**Cost**	**Date**	**Cost**	**Date**
Phase 1 OMN	500,000	February	250,000	January	500,000	February
Phase 2 OMN	1,000,000	August	500,000	August	1,000,000	August
Phase 2 OPN	TBD					
	SPAWAR					

AT/FP Investment in Pilot Programs

Information Management & Base Wide Alert

- CNRMA
- Leave-behind C4I capability (technology and CONOPs) supporting AT/FP and Emergency Management
- Leverage existing technologies
- Evaluate convergence of a solution-set capable of Navy-wide deployment
- Leverage other DoD programs
- Work toward convergence with civil agencies

Physical Security/Access Control

- CNRSE
- Identifying opportunities to reduce required manning/process layering/duplication of effort
  - –Smart Gate technology
  - –Waterside security system
  - –Perimeter intrusion detection system
  - –Perimeter surveillance

Physical Security/Access Control

- CNRSW
- Identifying opportunities to reduce required manning/process layering/duplication of effort
  - Vehicle and personnel access control to piers
  - Enclave personnel tracking
  - Incorporating technology for off-hour manning/monitoring
  - Smart Fence with Sensor back-up
  - Access to North Island

POA&M for Implementation of Ashore AT/FP Program

Short Term

- Align with Joint CBRN Programs across Regions
- Implement AT/FP Risk-Based Investment Strategy
- Fully develop SSG/SAT Organizations (N34/CNI)
- Initiate FY 04/05 Pilot Programs (CNI)
- Finalize Required Operational Capabilities (ROCs) and apply across the regions (FFC/CNI)
- Finalize Regional Capability Packages for Fleet Review (CNI)
- Establish Regional Navy Ashore AT/FP POM (CNI/SYSCOMS/Regions)
- Finalize Manpower Sourcing Strategy (CNI)

Mid Term

- Finalize and initiate Navy Ashore AT/FP Plan and Program (CNI)

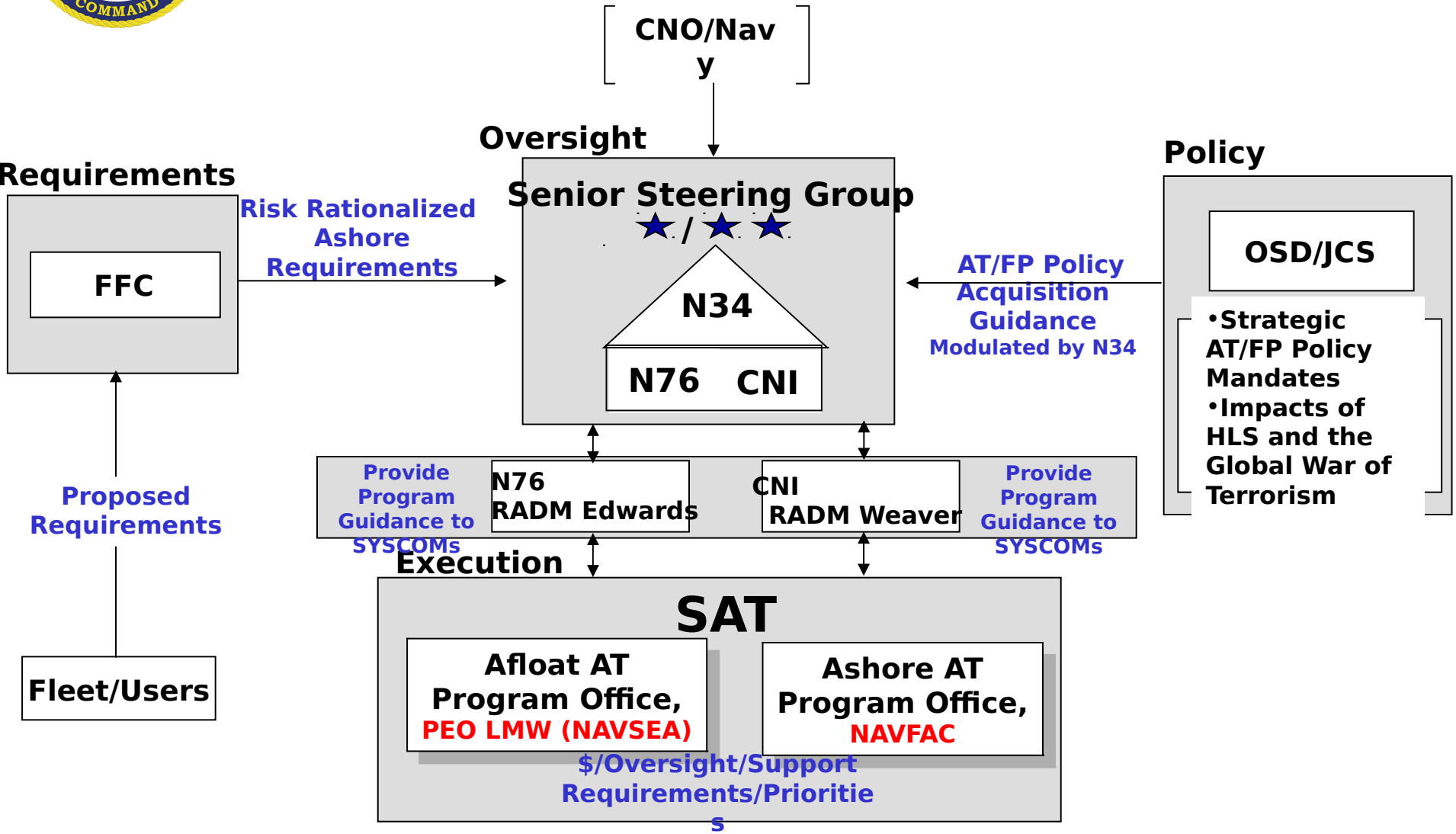
Long Term

- Implement world-wide FP Integrated Logistics Support Contract (CNI/NAVFAC)
- Continue Model Improvements (e.g. Value Deterrence, Capability Mapping)

QUESTIONS?

BACKUP

Senior Steering Group/SYSCOM Antiterrorism Team Approach to AT/FP Solutions



Assess Threat

Category	Scenario Relative Threat Assessment Criteria	Relative Threat Weighting
VH	This scenario is at least an order of magnitude more likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)	10
H	This scenario is at least twice as likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)	2
M	Default relative threat level for a "typical" scenario (Use this threat level unless the description for one of the relative threat levels is more fitting)	1
L	This scenario is at least half as likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)	0.5
VL	This scenario is at least an order of magnitude less likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)	0.1

Assess Vulnerability

Category	Vulnerability Assessment Criteria (including detection, security response, attack complexity, and target hardness considerations)	Likelihood of a Successful Attack After Initiation
VH	An attack would be defeated/unsuccessful less than 10 out of 100 times (Likelihood of successful attack: >90%)	0.9
H	An attack would be defeated/unsuccessful up to 1 out of 4 times (Likelihood of successful attack: 65% to 90%)	0.75
M	An attack would be defeated/unsuccessful up to 1 out of 2 times (Likelihood of successful attack: 35% to 65%)	0.5
L	An attack would be defeated/unsuccessful up to 3 out of 4 times (Likelihood of successful attack: 10% to 35%)	0.25
VL	An attack would be defeated/unsuccessful more than 90 out of 100 times (Likelihood of successful attack: <10%)	0.1

Assess Criticality

Criticality Assessment Criteria				Representative
Category	Death/Injury	Assets and	Mission Capability	
VH	>1,000 deaths or serious injuries *Benchmark Example* 9/11 World Trade Center attack	>$1 billion *Benchmark Example* 9/11 World Trade Center attack	Creates critical long-term vulnerabilities in *Benchmark Example* Destruction of multiple key military assets (e.g.,	$5,000,000,000
H	100 to 1,000 deaths or serious injuries *Benchmark Example* 9/11 attack on the Pentagon	$100 million to $1 billion *Benchmark Example* Destruction of an individual naval vessel	Creates critical short-term vulnerabilities in *Benchmark Example* Damage, but not destruction, to multiple	$500,000,000
M	10 to 100 deaths or *Benchmark Example* Attack on the USS Cole	$10 million to $100 *Benchmark Example* Destruction of an individual shore facility	Long-term disruptions in *Benchmark Example* Extended blockage of a strategic port or supply	$50,000,000
L	1 to 10 deaths or serious *Benchmark Example* Loss of staff at a small terminal or facility	$1 million to $10 million *Benchmark Example* Short-term repairable damage	Short-term disruptions *Benchmark Example* Temporary outage with available compensatory	$5,000,000
VL	No deaths or serious injuries; relatively only *Benchmark Example* Incident with only minor injuries	< $1 million *Benchmark Example* Other types of damage and mission interruption	No serious military/defense impact *Benchmark Example* Nuisance or inefficiency type impacts on military	$500,000

Strategy Components

- **Technology Insertion/CONOPS**
  - Continuous review, testing, adoption of state-of-the-art technology and concept of operations
- **Manpower Management**
  - Workload and staff modeling to reflect standard precepts of technology, CONOPS, ROC, and CL
- **Strategic Sourcing Policy Management**
  - Review controlling authorities, develop conforming strategies, and offer proposed revisions if prudent
- **Business Improvements**
  - Develop and coordinate programmatic and field initiatives to ensure efficient use of resources on a continuous basis

Recommendations

- Approve the concept of the Risk Based Investment Model
- Unless otherwise directed, pursue an approach of risk mitigation and management through rigorous analysis of technology, manpower, physical improvements, and C4I integration
  - Enhance AT/FP capabilities at shore installations, while accepting risk and reducing the cost of the overall AT/FP program